**CSCE 44303/54203 Homework 2**

**Release: September 6, 2024**

**Due: September 13, 2024**

**Full Grade: 122 pts**

**Note: If you use handwriting, please write clearly. Unrecognizable writing might cause loss of points.**

**Problem 1.** **(6 pts)** Classify each of the following as a violation of confidentiality, integrity, or authenticity. Choose the best match for each.

* Paul makes a copy of Linda’s private data.
* Gina modifies Roger’s homework solution.
* Henry spoofs Julie’s IP address to send a message to a computer.

**Problem 2. (6 pts)** For a cipher, if you use a 16-bit long key, what will be the problem?

**Problem 3. (10 pts)** One-time pad. (1) In one-time pad, suppose a one-byte message is 10111001, and the key is 10010011. Show the encryption process at the sender and the decryption process at the receiver. (2) Can an attacker in the network (between the sender and the receiver) do something over the ciphertext and cause the receiver to incorrectly decrypt the second bit in the message and, if so, how? (3) If one key is used to encrypt two different messages, what will be the problem?

**Problem 4. (6 pts)** Why can’t a block cipher have a smaller output (i.e., ciphertext block) size than the input (i.e., plaintext block) size?

**Problem 5. (10 pts)** Suppose a message has been encrypted using an old system with the basic DES algorithm under key k. (i) If the receiver of the message is running a new system with 3DES implemented. Can the receiver decrypt the ciphertext by setting k1=k2=k3=k and why? (ii) If the encryption of 3DES used the EEE mode instead of EDE and the decryption used the DDD mode instead of DED, can the receiver decrypt the ciphertext by setting k1=k2=k3=k and why?

**Problem 6.** **(12 pts)** In EDE mode of 3DES, encryption of message m with keys k1, k2 and k3 works as follows: C=**E**k1(**D**k2(**E**k3(m))), where E and D denote the encryption and decryption operation respectively. Given some <plaintext, ciphertext> pairs, how can an attacker find the three keys with effort in the order of 2112? Describe in details. (hint: meet-in-the-middle attack)

**Problem 7.** **(15 pts)** a. Suppose Alice shares a secret block cipher key, KAB with Bob, and a different secret block cipher key, KAC with Charlie. Describe a method for Alice to encrypt an m-block message such that it can only be decrypted with the cooperation of both Bob and Charlie. The ciphertext should only be a constant size greater than m blocks. For example, if the message size is 2m blocks, it doesn’t meet this requirement; if the message size is ~~2m+c~~ m+c blocks where c is a constant, it meets this requirement. You may assume that Bob and Charlie have a pre-established secret channel on which to communicate.

b. Now, suppose Alice shares a block cipher key, KAB with Bob, a block cipher key KAC with Charlie, and a block cipher key KAD with David. Describe a method for Alice to encrypt an m-block message such that any two of Bob, Charlie, and David can decrypt (for example, Bob and Charlie can decrypt), but none of them can decrypt the message themselves. Again, the ciphertext should only be a constant size greater than m blocks. (Hint: Pick a random message encryption key to encrypt the message with. Then add three ciphertext blocks to the ciphertext header.)

c. How does your solution from part (b) scale as we increase the number of recipients? In other words, suppose Alice has a secret key with each of n recipients and wants to encrypt so that any k out of n recipients can decrypt, but any k-1 cannot. What would be the length of the header as a function of n and k?

**Problem 8. (6 pts)** When using block cipher to encrypt a large message, padding is usually needed. Suppose Dr. Smart has designed a padding scheme, which will append a positive number of bytes of value “10101010” to the message until the padded message size is a multiple of the block size. Is this a good padding scheme and why?

**Problem 9. (9 pts)** For block cipher modes, under the ECB mode, if ten consecutive message blocks of the same message are the same, will their ciphertext blocks also be the same? How about in the CBC mode? How about in the Counter mode?

**Problem 10. (10 pts)** For the CBC mode: (1) If one IV value is used to encrypt two messages, what will be the problem? (2) Suppose a message is divided into five message blocks. If the third ciphertext block is modified during transit, which blocks can the receiver correctly decrypt and which not?

**Problem 11. (10 pts)** For the Counter mode, suppose a message is divided into five message blocks. (1) If the nonce part of the counter is modified during transit, which blocks can the receiver correctly decrypt and which not? (2) If the third ciphertext block is modified during transit, which blocks can the receiver correctly decrypt and which not?

**Problem 12.** **(10 pts)** Suppose public-key cryptography is used to encrypt the communications between Alice and Bob. Alice’s public key is eA, private key is dA; Bob’s public key is eB, private key is dB. Now Alice wants to send a message m to Bob. (1) Can Alice encrypt the message using key dB and why? (2) Can Alice encrypt the message using key dA and why?

**Problem 13. (12 pts)** Alice’s RSA parameters are . Bob’s RSA parameters are . Suppose Alice wants to send a message m=3 to Bob, and protect the confidentiality of the message with RSA encryption. Show how Alice will encrypt the message and how Bob will decrypt the message.